APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/451,254	11/29/1999	YACOV YACOBI	MS1-306US	8800

22801   7590   06/21/2002

LEE & HAYES PLLC
421 W RIVERSIDE AVENUE SUITE 500
SPOKANE, WA 99201

EXAMINER
WINTER, JOHN M

ART UNIT	PAPER NUMBER
3621	

DATE MAILED: 06/21/2002

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 07-01)

	Application No.		Applicant(s)
Office Action Summary	09/451,254		YACOBI ET AL.
	Examiner		**Art Unit**
	John M Winter		3621

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☐ Responsive to communication(s) filed on _____ .

2a) ☐ This action is **FINAL**.   2b) ☒ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) *1-60* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) ☒ Claim(s) *31-41* is/are allowed.

6) ☒ Claim(s) *1-30 and 51-60* is/are rejected.

7) ☐ Claim(s) _____ is/are objected to.

8) ☒ Claim(s) *42-50* are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.

10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11) ☐ The proposed drawing correction filed on _____ is: a) ☐ approved b) ☐ disapproved by the Examiner.

    If approved, corrected drawings are required in reply to this Office action.

12) ☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a) ☐ All b) ☐ Some * c) ☐ None of:

      1. ☐ Certified copies of the priority documents have been received.

      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .

      3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage
          application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

    a) ☐ The translation of the foreign language provisional application has been received.

15) ☒ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .

4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: .

DETAILED ACTION

Election/Restrictions

Restriction to one of the following inventions is required under 35 U.S.C. 121:

I.   Claims 1-42, 51- 60, drawn to a method of managing electronic assets, classified in class 705, subclass 69.

II. Claim 42-50, are drawn to a method of using electronic coupons, classified in class 705, subclass 14.

The inventions are distinct, each from the other because of the following reasons:

Inventions I and II are related as combination and subcombination. Inventions in this relationship are distinct if it can be shown that (1) the combination as claimed does not require the particulars of the subcombination as claimed for patentability, and (2) that the subcombination has utility by itself or in other combinations (MPEP § 806.05(c)). In the instant case, the combination as claimed does not require the particulars of the subcombination as claimed because a method using electronic coupons, as stated in invention II has no dependency on a method of managing electronic assets as stated in invention I. The subcombination has separate utility such as promoting customer loyalty.

Because these inventions are distinct for the reasons given above and have acquired a separate status in the art as shown by their different classification, restriction for examination purposes as indicated is proper.

During a telephone conversation with Lewis Lee on May 29, 2002 a provisional election was made with traverse to prosecute invention I, claims 15-17. Affirmation of this election must be made by applicant in replying to this Office action. Claims 42-50 are withdrawn from further consideration by the examiner, 37 CFR 1.142(b), as being drawn to a non-elected invention.

Claims 1-42, 51-60 have been examined

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) do not apply to the examination of this application as the application being examined was not (1) filed on or after November 29, 2000, or (2) voluntarily published under 35 U.S.C. 122(b). Therefore, this application is examined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

Claims 1,2,3,10,11,24,25-30 and 57 are rejected under 35 U.S.C. 102(e) as being unpatentable over Briscoe (US Patent 6,341,273).

As per claim 1, 10 and 11.

Briscoe ('273) discloses a method comprising:

minting a stick of electronic assets by digitally signing with an issuer's signature a composite of user-provided data items including a user identity. a bottom asset from a bottom of the stick. and a length of the stick:(column 5, lines 44-49)

spending one or more assets from the stick at one or more vendors, wherein each expenditure with a particular vendor involves digitally signing with a user's signature a first asset from the stick to be spent and passing the user-signed first asset along with the issuer-signed composite to the particular vendor for verification and subsequently passing any additional assets to be spent without user signature to the particular vendor;(column 1, lines 63-67; column 2, lines 1-24)

depositing one or more assets collected by the particular vendor by digitally signing with the particular vendor's signature a composite of data items including ,4 the user-signed first asset and a last asset spent by the user from the stick and ,; passing the vendor-signed composite along with the issuer-signed composite to the issuer. (column 6, lines 21-46)

Claims 10 and 11 are in parallel with claim 1.

As per claim 2,

Briscoe ('273) discloses a method as recited in claim 1,

further comprising storing the stick of electronic assets in a tamper-resistant electronic wallet. (column 7, lines 60-65)

As per claim 3,

Briscoe ('273) discloses a method as recited in claim 1,

further comprising storing the stick of electronic assets in an electronic wallet constructed with a secure-processor architecture. (column 8, lines 6-11).

As per claim 24, 27,28,29 and 30

Briscoe (273) discloses a method for issuing electronic assets, comprising:

creating, at a user, a stick of L electronic assets by computing: $C_i = h^i(x)$ (for $i=1,\ldots\ldots,L$) where $h(x)$ is a hashing function of the value x (figure 3;also column 3, lines 54-55)

submitting a withdrawal request from the user to an issuer, the withdrawal request having a user identity U, a last asset value CI, taken from a bottom of the stick, and the value L, while omitting any vendor identity signing, at the issuer, the withdrawal request; returning the signed withdrawal request to the user. ;(column 6, lines 20-46)

Claims 27,28,29 and 30 are in parallel with claim 24

As per claim 25,
Briscoe (273) discloses a method as recited in claim 24,
further comprising storing the stick of electronic assets and signed withdrawal request in
a tamper-resistant electronic wallet.(column 7, lines 60-65)

As per claim 26,
Briscoe (273) discloses a method as recited in claim 24,
further comprising storing the stick 2 of electronic assets and signed withdrawal request
in an electronic wallet constructed with a secure-processor architecture.(column 8, lines6-11)

As per claim 57,
Briscoe (273) discloses an electronic wallet having memory and a processor, the
electronic wallet being programmed to create a stick of L electronic assets by computing: $C_i =$
$h^i(x)$ (for $i=1,......,L$) where h(x) is a hashing function of a value x;(Abstract)
form a withdrawal request having a user identity U. a last asset value C_L, taken from a
bottom of the stick, and the value L, while omitting any vendor identity; submit withdrawal
request to an issuer and receive the withdrawal request back with an issuer signature to store the
signed withdrawal request and the stick. (column 6, lines 20-46)

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all
obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in
> section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are
> such that the subject matter as a whole would have been obvious at the time the invention was made to a person
> having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the
> manner in which the invention was made.

Claims 4,15 and 54 are rejected under 35 U.S.C. 103(a) as being unpatentable over
Briscoe (US Patent 6,341,273) as applied to claim 1,claim 12 and claim 51, and further in view
of Chaum (US Patent 5,878,140).

As per claim 4,
Briscoe ('273) discloses a method as recited in claim 1,
Wherein the minting compromises minting the stick of assets. (column 5, lines 27-49)
Briscoe ('273) does not explicitly disclose using a blind signature protocol, Chaum ('140)
discloses using a blind signature protocol, It would have been obvious to one having ordinary
skill in the art at the time the invention was made to combine the Briscoe ('273) method with the

Chaum ('140) method in order to mint sticks of assets with a blind signature protocol in order to protect user confidentiality.

As per claim 15,

Briscoe ('273) discloses a method as recited in claim 12,

wherein the forming comprises issuing the stick of assets. (column 5, lines 27-49)

Briscoe ('273) does not explicitly disclose using a blind signature protocol, Chaum ('140) discloses using a blind signature protocol, It would have been obvious to one having ordinary skill in the art at the time the invention was made to combine the Briscoe ('273) method with the Chaum ('140) method in order to mint sticks of assets with a blind signature protocol in order to protect user confidentiality.

Claim 54 is rejected under 35 U.S.C. 103(a) as being unpatentable over Briscoe (US Patent (6,341,273) and further in view of Chaum (US Patent 5,878,140)

As per claim 54,

Briscoe (273) discloses an electronic asset system as recited in claim 51,

Briscoe (273) does not specifically disclose wherein the issuer wallet signs the composite using a blind signature protocol. Chaum ('140) discloses the issuer wallet signs the composite using a blind signature protocol. It would be obvious to one of ordinary skill in the art at the time of the invention to utilize a blind signature protocol because this prevents adversaries from gaining illicit information about the consumer.

Claim 5 is rejected under 35 U.S.C. 103(a) as being unpatentable over Briscoe (US Patent 6,341,273) as applied to claim 1 above and further in view of Official notice.

As per claim 5,

Briscoe ('273) discloses a method as recited in claim 1, wherein the spending comprises:

concatenating a vendor identity with the first asset from the stick to form a payment request; (column 6, lines 33-37)

submitting the user-signed payment request along with the issuer-signed withdrawal request to the vendor; (column 6, lines 33-37)

accepting the first asset as payment in an event that the user and the issuer are verified;(column 6, lines 40-43)

subsequently passing any additional assets from the stick as payment to the vendor without digitally signing them with the user's signature;(column 6, lines 49-59)

Official Notice is taken that "signing the payment request with a signature of the user" is common and well known in prior art in reference to electronic money. It would have been obvious to one having ordinary skill in the art at the time the invention was made to sign the payment request with the signature of the user in order to provide verification of the users identity.

Claims 7, 8,9,19 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Briscoe (US Patent 6,341,273) as applied to claim 1 and claim 12 and further in view of Yacobi (US Patent 5,878,138).

As per claim 7,
Briscoe ('273) discloses a method as recited in claim 1,
Briscoe ('273) does not explicitly disclose further comprising auditing the assets deposited by the vendor. Yacobi ('138) discloses auditing the assets deposited by the vendor. It would have been obvious to one having ordinary skill in the art of electronic transactions at the time the invention was made to combine the Briscoe ('273) method with the Yacobi ('138) method in order to guarantee the validity of the data specified by the vendor.

As per claim 8
Briscoe ('273) discloses a method as recited in claim 1,
Briscoe ('273) does not explicitly disclose further comprising auditing a sample
of the assets paid by the user to the vendor. Yacobi ('138) discloses further comprising auditing a sample of the assets paid by the user to the vendor. It would have been obvious to one having ordinary skill in the art of electronic transactions at the time the invention was made to combine the Briscoe ('273) method with the Yacobi ('138) method in order to guarantee the validity of the data specified by the vendor.

As per claim 9
Briscoe ('273) discloses a method as recited in claim 1,
Briscoe ('273) does not explicitly disclose further comprising selecting, at the vendor, a subset of less than all of the assets paid by the user to the vendor and submitting the subset of assets to an auditor for fraud evaluation. Yacobi ('138) discloses further comprising selecting, at the vendor, a subset of less than all of the assets paid by the user to the vendor and submitting the subset of assets to an auditor for fraud evaluation. It would have been obvious to one having ordinary skill in the art of electronic transactions at the time the invention was made to combine the Briscoe ('273) method with the Yacobi ('138) method in order to guarantee the validity of the data specified by the vendor.

As per claim 19,
Briscoe ('273) discloses a method as recited in claim 12,
Briscoe ('273) does not explicitly disclose further comprising auditing the assets from the first and second runs of assets for fraud. Yacobi ('138) discloses auditing the assets from the first and second runs of assets for fraud. It would have been obvious to one having ordinary skill in the art of electronic transactions at the time the invention was made to combine the Briscoe ('273) method with the Yacobi ('138) method in order to guarantee the validity of the data specified by the vendor.

As per claim 20
Briscoe ('273) discloses a method as recited in claim 12,
Briscoe ('273) does not explicitly disclose further comprising auditing a

sample of assets from the first and second runs of assets for fraud. Yacobi ('138) discloses further comprising auditing a sample of assets from the first and second runs of assets for fraud. It would have been obvious to one having ordinary skill in the art of electronic transactions at the time the invention was made to combine the Briscoe ('273) method with the Yacobi ('138) method in order to guarantee the validity of the data specified by the vendor.

Claims 12,13,14,16,18,21,22 and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Briscoe (US Patent 6,341,273) and further in view of Official Notice.

As per claim 12, 22, and 23.

Briscoe ('273) discloses a method for issuing electronic assets, comprising:
forming a stick of L electronic assets C; (for i=1, , L) where each asset can be derived from a preceding asset in the stick;(Abstract)
signing the stick with a signature of a party issuing the assets;
spending a first run of one or more assets from the stick at a first vendor;(column 1, lines 63-67; column 2, lines 1-24)

Official Notice is taken that "spending a second run of one or more assets from the stick at a second vendor" is common and well known in prior art in reference to electronic money. It would have been obvious to one having ordinary skill in the art at the time the invention was made to utilize electronic assets at a plurality of vendors.

Claims 22 and 23 parallel claim 12.

As per claim 13.

Briscoe ('273) discloses a method as recited in claim 12,
further comprising storing the stick of electronic assets in a tamper-resistant electronic wallet.(column 7, lines 60-65)

As per claim 14,

Briscoe ('273) discloses a method as recited in claim 12,
further comprising storing the stick to of electronic assets in an electronic wallet constructed with a secure-processor architecture.(column 8, lines 6-11)

As per claim 16,

Briscoe ('273) discloses a method as recited in claim 12, wherein the forming comprises:
creating the stick of L electronic assets by computing $C_i = h^i(x)$ (for $i=1,......,L$) where $h(x)$ is a one way hashing function of the value x (figure 3;also column 3, lines 54-55)

As per claim 18,

Briscoe ('273) discloses a method as recited in claim 12, wherein the spending comprises:
submitting the user-signed asset along with the signed stick to the first vendor;(column 6, lines 33-37)

in an event the first asset is accepted, subsequently submitting any additional assets from the stick without digitally signing them. (column 6, lines 49-59)

Official Notice is taken that "signing the payment request with a signature of the user" is common and well known in prior art in reference to electronic money. It would have been obvious to one having ordinary skill in the art at the time the invention was made to sign the payment request with the signature of the user in order to provide verification of the users identity.

As per claim 21
Briscoe ('273) discloses a method as recited in claim 12,
further comprising depositing the first and second runs of assets.
Official Notice is taken that "depositing the first and second runs of assets" is common and well known in prior art in reference to electronic money. It would have been obvious to one having ordinary skill in the art at the time the invention was made to deposit assets in order to profit from prior sales of items.

Claim 51- 53 are rejected under 35 U.S.C. 103(a) as being unpatentable over Briscoe (US Patent 6,341,273) and further in view of Schneier (Applied Cryptography, Protocols, Algorithms, and source code in C)

As per claim 51,
Briscoe (273) discloses an electronic asset system comprising:
an issuer wallet having a processor and storage, the issuer wallet digitally signing with an issuer's signature a composite of user-provided data items including a user identity, a bottom asset from a bottom of a stick of electronic assets, and a length of the stick(column 5, lines 27-49);
a user wallet having a processor and storage to store the stick of electronic assets and issuer-signed composite and to spend one or more assets from the stick at one or more vendors,(column 7, lines 60-65)
the user wallet spending one or more assets by digitally signing with a user's signature a first asset from the stick to be spent and passing the user-signed first asset along with the issuer-signed composite to the vendor for verification; whereupon verification, the user wallet subsequently passes any additional assets to be spent without user signature to the vendor;(column 6, lines 21-46)
a vendor wallet having a processor and storage to store one or more assets spent by the user wallet, the vendor wallet depositing the assets collected from the user wallet by digitally signing with the particular vendor's signature a composite of data items including the user-signed first asset and a last asset passed in the stick received from the user wallet (column 6, lines 33-45)
Briscoe (273) does not specifically disclose passing the vendor-signed composite along with the issuer-signed composite to the issuer wallet for verification. Schneier discloses passing the vendor-signed composite along with the issuer-signed composite to the issuer wallet.(page 51 – "Key and message transmission" It would be obvious to one of ordinary skill in the art at the

time of the invention combine the Briscoe method with Schneier's teaching of message transmission in order to prevent adversaries from forging electronic asset transactions.

As per claim 52,
Briscoe (273) discloses an electronic asset system as recited in claim 51
wherein the issuer wallet, the user wallet, and the vendor wallet are tamper-resistant. (column 7,lines 60-65)

As per claim 53,
Briscoe (273) discloses an electronic asset system as recited in claim 51,
wherein the issuer wallet, the user wallet, and the vendor wallet are tamper-resistant constructed with a secure-processor architecture. (column 8,lines 6-11)

Claims 55 is rejected under 35 U.S.C. 103(a) as being unpatentable over Briscoe (US Patent (6,341,273) and further in view of Deemers (US Patent 6,021,399)

As per claim 55,
Briscoe (273) discloses an electronic asset system as recited in claim 51,
Briscoe (273) does not specifically disclose further comprising an auditing system to audit the electronic assets to detect whether assets have been used in a fraudulent manner.
Deemers et al. discloses an auditing system to audit the electronic assets to detect whether assets have been used in a fraudulent manner.(column 13, lines 62-67; column 14, lines 1-10) It would be obvious to one of ordinary skill in the art at the time of the invention to combine Briscoe's electronic asset system with Deemer et al's teaching of an auditing system in order to reduce the vendors risk of losing money due to illicit transactions.

As per claim 56,
Briscoe (273)discloses an electronic asset system as recited in claim 51,
Briscoe (273) does not specifically disclose a probabilistic auditing system to sample a subset of less than all electronic assets, to detect whether assets have been used in a fraudulent manner. Deemers et al. discloses a probabilistic auditing system to sample a subset of less than all electronic assets, to detect whether assets have been used in a fraudulent manner..(column 13, lines 62-67; column 14, lines 1-10) It would be obvious to one of ordinary skill in the art at the time of the invention to combine Briscoe's electronic asset system with Deemer et al's teaching of an auditing system in order to reduce the vendors risk of losing money due to illicit transactions.

Claims 59 and 60 are rejected under 35 U.S.C. 103(a) as being unpatentable over Briscoe (US Patent 6,341,273) and further in view of Yacobi (US Patent 5,878,138).

As per claim 59
Briscoe (273) discloses an electronic wallet having memory and a processor,
Briscoe ('273) does not explicitly disclose the electronic wallet being programmed to:
receive a run of assets from a user;

select a subset of less than all of the assets received from the user;

submit the subset of assets to an auditor for evaluation of fraudulent expenditure.

Yacobi ('138) discloses the electronic wallet being programmed to:

receive a run of assets from a user;

select a subset of less than all of the assets received from the user;

submit the subset of assets to an auditor for evaluation of fraudulent expenditure. It would have been obvious to one having ordinary skill in the art of electronic transactions at the time the invention was made to combine the Briscoe ('273) method with the Yacobi ('138) method in order to guarantee the validity of the data specified by the vendor.

As per claim 60,

Briscoe (273) discloses an electronic wallet as recited in claim 59,

Briscoe ('273) does not explicitly disclose further programmed to randomly select the subset of assets.

Yacobi ('138) discloses programmed to randomly select the subset of assets.(column 3, lines 30-36)

It would have been obvious to one having ordinary skill in the art of electronic transactions at the time the invention was made to combine the Briscoe ('273) method with the Yacobi ('138) method in order to guarantee the validity of the data specified by the vendor.

Allowable Subject Matter

Claims 31-33, 34-40 are allowed

Claims 6, 17, 58 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims and complying with double patenting statutes.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- Maytas (US Patent 5,231,666) Cryptographic method for updating financial records.

- Deemers et al (US Patent 5,952,638) Space efficient method of electronic payments.

- Mjolsnes et al. (US Patent 5,905,976) System of secured payment by the transfer of electronic money theough an interbank network

- Yacobi (US Patent 5,511,121) Efficient electronic money

Any inquiry concerning this communication or earlier communications from the examiner should be directed to John M Winter whose telephone number is (703) 305-3971. The examiner can normally be reached on M-F 8:30-6, 1st Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, James P Trammel can be reached on (703)305-9768. The fax phone numbers for the organization where this application or proceeding is assigned are (703) 305-7687 for regular communications and (703) 305-7687 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 308-1113.

***

June 11, 2002

JAMES P. TRAMMELL
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 3600